

1

cdgrf 43

2

3

4

## Smart Card

5

### Stage 1 Description

6

**(Version 1.1)**

7

**May 22, 1996**

8

**CDMA Development Group**

9

**Smart Card Team Document**

10

11

12

13

14

15

**Please contact:**

16

**Narisa Chu, Comcast Cellular, Wayne, PA**

17

**610-995-5278, Fax: -5224**

18

**METROPHONE/WAYNE/NCHU%Comcast\_Metrophone@mciemail.com**

19

**Cheryl Johnson U S Cellular, Chicago, IL**

20

**312-399-8964 Fax: -4984**

21

**Cheryl\_Johnson\_at\_USCC\_\_P3@cellular.uscc.com**

1		
2	<b>1. INTRODUCTION</b>	<b>3</b>
3	<b>2. REFERENCES</b>	<b>5</b>
4	<b>2.1. References for Smart Card</b>	<b>5</b>
5	<b>3. DEFINITIONS</b>	<b>6</b>
6	<b>4. GLOBAL FEATURE DESCRIPTION</b>	<b>8</b>
7	<b>5. SMART CARD FEATURE DESCRIPTIONS</b>	<b>9</b>
8	<b>5.1. Pre-paid Service</b>	<b>9</b>
9	5.1.1. Normal Procedures With Successful Outcome	11
10	5.1.2. Exception Procedures or Unsuccessful Outcome	12
11	5.1.3. Alternate Procedures	13
12	5.1.4. Interactions With Other Wireless Services	13
13	<b>5.2. Plastic Roaming Service</b>	<b>14</b>
14	5.2.1. Normal Procedures With Successful Outcome	15
15	5.2.2. Exception Procedures or Unsuccessful Outcome	16
16	5.2.3. Alternate Procedures	17
17	5.2.4. Interactions With Other Wireless Services	17
18	<b>5.3. Fraud Prevention Service</b>	<b>18</b>
19	5.4.1. Normal Procedures With Successful Outcome	19
20	5.4.2. Exception Procedures or Unsuccessful Outcome	20
21	5.4.3. Alternate Procedures	21
22	<b>5.4. Future Services</b>	<b>22</b>
23	5.5.1. Portable Storage	22
24	5.5.2. Non-Telephony	23
25		

1

2

## 1. Introduction

---

3

4

5

6

This document presents Stage 1 descriptions for CDMA smart card services. The intent of this document is to provide inputs on user considerations, and possible service interactions to aid in the development of smart card services and other layer associated capabilities.

7

Smart card functionality includes:

8

9

10

- Privacy key management and authentication interface between the subscriber and the CDMA mobile station
- Personalized feature subscription record
- Transport of non-telephony applications, e.g. credit card, electronic coin purse and loyalty program
- Remote management of data/voice/facsimile applications.

11

12

Smart card applications are identified below:

13

14

15

16

17

18

19

20

21

- Pre-paid Services
- Plastic Roaming
- Fraud Prevention
- Future applications: Portable Storage and Non-telephony Services

It is assumed one card per subscription at the initial stage. Ultimately, there can be multiple cards per subscriber and the smart card can enable the wireless data/voice services as the transport mechanism underlying non-telephony, end-to-end applications.

22

23

With the above functions and applications, service providers will be able to realize the following benefits:

24

25

26

27

28

- 1) Service offers with billing and provisioning capabilities through an intelligent/synergistic mechanism.
- 2) Common/flexible means for billing and provisioning cross wireline, wireless, and cable TV services.
- 3) Plastic roaming cross different access technology networks.

1           4) Service portability for subscribers, subscriptions, network technologies, and service  
2           providers.

3           5) Marketing differentiation - Brand exposure, expanded distribution channels,  
4           advertising revenues, customer loyalty programs.

5           6) Billing and customer care alternatives - Fraud protection/management, ease of  
6           distribution, remote activation alternative.

7           7) Cheaper to subsidize if needed: cost per card is much cheaper than cost per mobile  
8           station.

9           8) Revenue assurance with pre-paid service.

10          The smart card can bring the following benefits to the subscribers:

11          1) Convenience for international business travel with rental mobile stations.

12          2) Domestic travel to areas with different network technology.

13          3) Public mobile stations with individual billing report.

14          4) Employees can share mobile stations with personalized privileges and accounting.

15          5) Family members can share a mobile station with cards tailored to specific needs and  
16           individual accounting.

17          6) It is easier to carry a plastic card than a mobile station.

18          7) Theft-proof : a smart card can not be used without a CHV verification and other  
19           security mechanism built in the network, e.g. IS-41 CAVE, etc.

20          8) Effective fraud control and prevention.

2 

## 2. References

---

3 

### 2.1. References for Smart Card Services

---

5 International Standards Organization (ISO) 7816-1,2,3-6 *Information*  
6 *technology - Identification cards - Integrated circuit(s) cards with contact parts*  
7 **1 through 6**

8 **T1P1.3/V. 5. PCS User Identity Module (UIM) Specification, 1996**

9 CCITT 1988 (Blue Book), Volume III - Fascicle III.7, *Integrated Services Digital*  
10 *Network (ISDN) General Structure and Service Capabilities; Recommendations*  
11 **I.110 - I.257.**

12 Technical Specification GSM 02.17: *Subscriber Identity Module, Functional*  
13 *Characteristics; August 31, 1993.*

14 Technical Specification GSM 11.11: *Specification of the Subscriber Identity*  
15 *Module - Mobile Equipment (SIM - ME) interface; October 1993.*

16 J-STD-007, **PCS 1900 Smartcard - ANSI Standard**

17 J-STD-008-1995, **Personal Station-Base Station Compatibility**

18 ANSI Requirements for 1.8 to 2.0 GHz Code Division Multiple Access (CDMA)  
19 Personal Communications Systems, *Telecommunications Industry Association,*  
20 **1995.**

21 TIA/EIA/IS-41-C, *Cellular Radio-Telecommunications Intersystem Operations,*  
22 *Telecommunications Industry Association, December 1995.*

23 TIA/EIA/IS-95-A, *Mobile Station-Base Station Compatibility Standard for Dual-*  
24 *Mode Wideband Spread Spectrum Cellular System, Telecommunications Industry*  
25 *Association, May 1995.*

26 TIA/EIA/IS-95-A, *Appendix A, Message Encryption and Voice Privacy. An ITAR*  
27 *controlled document subject to restricted distribution. Contact the*  
28 *Telecommunications Industry Association, Washington, D.C., November 16, 1994.*

29 TSB50, *User Interface for Authentication Key Entry, Telecommunications*  
30 *Industry Association, March 1993.*

31 TSB74, *Support for 14.4 kbps Data Rates and PCS Interaction for Wideband*  
32 *Spread Spectrum Cellular Systems, Telecommunications Industry Association,*  
33 *December 1995.*

### 3. Definitions

---

3      **Authentication** - A secure procedure used to validate a mobile station's identity  
4      involving the A-key and the CAVE Algorithm.

5      **Authentication Center** - An entity that manages the authentication information related  
6      to the mobile station.

7      **Authentication Key (A-key)** - A secret 64-bit pattern stored in the subscriber unit. It is  
8      used to generate and update the subscriber unit's Shared Secret Data. The A-key is used  
9      in the authentication process.

10     **Authenticating Network** - Networks that validate a subscriber through authentication.

11     **Authorized Dealer** - An agent that is authorized by a service provider to sell that  
12     service provider's product or service to a customer.

13     **Automatic Teller Machine (ATM)**

14     **Call** - A temporary communication between telecommunications users for the purpose of  
15     exchanging information. A call includes the sequence of events that allocates and  
16     assigns resources and signaling channels required to establish a communications  
17     connection.

18     **Card Holder Verification (CHV)** - Access condition used by the SIM for the  
19     verification of the identity of the user.

20     **Cellular Service Provider** - A licensee of the responsible government agency (in the  
21     U.S., a licensee of the Federal Communications Commission) authorized to provide  
22     Cellular Radiotelephone Service.

23     **Code Division Multiple Access (CDMA)** - A technique for spread-spectrum multiple-  
24     access digital communications that creates channels through the use of unique code  
25     sequences.

26     **Country Code** - A unique 1-, 2- or 3-digit code assigned to countries in the World  
27     Numbering Plan. For international dialing purposes, the world is divided into nine  
28     zones. The first digit of a country code is the world number.

29     **Customer** - A person who purchases a mobile station and is a prospective subscriber to  
30     a cellular service provider.

31     **Customer Service Center** - An entity of a service provider that provides user support  
32     and assistance to subscribers.

33     **Customer Service Representative** - A person that operates from a customer service  
34     center and provides user support and assistance to subscribers.

35     **DMH - Data Message Handler**

36     **Digits** - Digits consist of decimal integers 0, 1, 2, 3, 4, 5, 6, 7, 8 and 9.

37     **Distribution Channel** - A method for providing a product or service to a specific  
38     market.

39     **Directory Number** - The phone number used to dial a subscriber.

40     **Dual-mode Mobile Station** - A mobile station capable of analog or digital operation.

41     **Electronic Serial Number (ESN)** - A 32-bit number assigned by the mobile station  
42     manufacturer used to identify a mobile station. The ESN is unique for each legitimate  
43     mobile station.

44     **Home Location Register (HLR)** - The location register or database to which a MIN is  
45     assigned for record purposes such as subscriber information.

46     **International Mobile System Identification (IMSI)** - The information which uniquely  
47     identifies a subscriber to the PSTN or PLMN.

48     **Mobile Identification Number (MIN)** - The 10-digit number that represents the phone  
49     number of the subscriber unit.

1                   **Mobile Station (MS)** - The mobile or portable subscriber radio telephone equipment  
2                   (same as Cellular Subscriber Station).  
3                   **Mobile Switching Center (MSC)** - A configuration of equipment that provides cellular  
4                   radiotelephone service.  
5                   **National Number** - The number identifying a subscriber line or terminal within an area  
6                   designated by a country code.  
7                   **Network** - The telecommunications equipment that has any part in processing a call or  
8                   a supplementary service for the subscriber referred to. It may include local exchangers  
9                   and transit exchanges, but does not include the mobile station and is not limited to the  
10                  "public network" or any other particular set of equipment.  
11                  **NDSS** - Network Directed Systems Selection  
12                  **Numeric Assignment Module (NAM)** - The electronic memory module of the  
13                  subscriber unit where the MIN and other subscriber specific parameters are stored.  
14                  Subscriber units that have multi-NAM features offer users the option of using their units  
15                  in several different markets by registering with a local number in each location.  
16                  **OTASP** - Over-the-Air Service Provisioning  
17                  **PCS** - Personal Communication Services  
18                  **Personal Identification Number (PIN)** - A string of digits used to validate a  
19                  subscriber's identity. In order to distinguish the PIN from the de-registration or de-  
20                  activation feature codes using a Modifier Digit "0," the PIN shall not start with the  
21                  digit 0. The PIN shall be at least 4 digits and shall not have too many repeated digits.  
22                  (e.g., no more than 2).  
23                  **Portability** - The ability for a smart card to operate in a variety of smart card compatible  
24                  terminals.  
25                  **PLMN** - Public Land Mobile Network  
26                  **PSTN** - Public Switch Telephone Network  
27                  **Registration** - Method by which a mobile station notifies the network of its location and  
28                  parameters.  
29                  **Roamer** - A mobile station operating in a cellular system or network other than the  
30                  one from which service is subscribed.  
31                  **Roamer Service Profile** - The specific set of features, capabilities and/or operating  
32                  restrictions, other than financial accountability, associated with the subscriber.  
33                  **Service Provider** - A company, organization, business, etc. which sells, administers,  
34                  maintains, and charges for the service. The service provider may or may not be the  
35                  provider of the network.  
36                  **Shared Secret Data(SSD)** - A 128-bit pattern stored in the mobile station (in semi-  
37                  permanent memory) and known by the network. The SSD is a concatenation of two 64-  
38                  bit subsets: SSD\_A which is used to support the authentication procedures and SSD\_B  
39                  which serves as one of the inputs to the process generating the encryption mask.  
40                  **Subscriber Identification Module (SIM)** - The SIM card is the Subscriber Identity  
41                  Module. It contains necessary information to verify and authenticate the subscriber.  
42                  There are two sizes, full size and plug-in.  
43                  **Smart Card Serial Number** - In order for the service providers to identify the smart  
44                  card, there needs to be a smart card serial number. This is a unique number that  
45                  identifies the smart card. It can be printed on the card. It is not secret data, it is not sent  
46                  over the air.  
47                  **Stage 1** - This stage is part of the overall method used to characterize  
48                  telecommunication services. Stage 1 defines the service aspects of a capability.  
49                  Specifically, Stage 1 provides a service description of a telecommunication service from  
50                  the user point of view (refer to CCITT Recommendation I.130).  
51                  **Stage 2** - This stage is part of the overall method used to characterize  
52                  telecommunication services. Stage 2 defines the functional aspects of a capability.  
53                  Specifically, Stage 2 provides a description of the functions at the user-network interface

1 and inside the network between network elements (refer to *CCITT Recommendation*  
2 *I.130*).

3 Stage 3 - This stage is part of the overall method used to characterize  
4 telecommunication services. Stage 3 defines the network implementation aspects of a  
5 capability. Specifically, Stage 3 provides a description of the actual protocols and  
6 formats used to develop the telecommunication service (refer to *CCITT*  
7 *Recommendation I.130*).

8 **Subscriber** - A person authorized for a feature or service.

9 **Subscriber unit (SU)** - The portion of the mobile or portable subscriber radiotelephone  
10 equipment that contains the unique information to identify a subscriber. The SU can be  
11 the entire mobile station itself, or a smart card or other device that contains such  
12 information.

13 **Universal Identification Module (UIM)** - This term is used in T1P1.3 to refer to the  
14 logic function or the SIM card in the mobile station.

15 **World Numbering Plan** - A plan created by the CCITT that provides each telephone  
16 subscriber with a unique number. Each world telephone number consists of a country  
17 code followed by the national number as defined in *CCITT Recommendations E.164*. By  
18 international agreement, the number of digits in the country code plus national number  
19 is limited to a tOTASPI of 12 digits currently, with a recommendation to increase the  
20 maximum length to 15 digits by the end of 1996.

21 **Validation** - The process by which a subscriber is authorized to access and use a cellular  
22 network.

23 **Verification** - The method used by a service provider to determine the credit of a new  
24 subscriber.

25

## 26 **4. Global Feature Description**

---

27 Upon the receipt of a smart card from a service provider, the subscriber shall be  
28 responsible for inserting the smart card into a mobile station or a smart card compatible  
29 device.

30 The subscriber with a smart card may have to subject to Card Holder Verification (CHV)  
31 (e.g. use of a Personal Identification Number - PIN) in order to access voice/data  
32 applications. Each smart card shall have a CHV to secure card access. Use of CHV is  
33 implementation specific.

34 The subscriber may use a single smart card containing multiple applications in multiple  
35 smart card compatible devices, provided the device supports the particular application.  
36 For example, a multi-application card supporting a telephony and a banking application  
37 may be successfully used in both a mobile station and an ATM-type machine.

38 The smart card can be removed from the mobile station when not in use. The size of a  
39 smart card does not have to be smaller than the mobile station as long as a compatible  
40 interface is provided. Full size smart cards are preferred because they can be removed  
41 from the mobile station and stored elsewhere with other payment type cards and used for  
42 other horizontal applications.

43 A normal phone call should not be allowed without the smart card present in the mobile  
44 station. There are exceptions to this case which will be determined and authorized by the

1 service provider. Examples are emergency 911 calls, calls to update the value of the  
2 individual account, 800 calls, service order calls, etc. When the smart card is inserted,  
3 the mobile station can be powered up manually or automatically.

4 It is assumed one card per subscription in this document.

## 5 6 **Smart Card Feature Descriptions**

---

7 The following sections describe individual smart card features and services.

### 8 **5.1. Pre-paid Service**

---

9 Pre-paid subscription will provide an attractive payment option to service providers as  
10 well as to a large segment of the customers because it can provide a means for "cash  
11 economy" and for poor credit, high risk customers to obtain wireless service.

12 A smart card can be used to support pre-paid subscription similar to a debit card. The  
13 subscriber can pay cash or link the smart card to an authorized credit card institute. The  
14 activation of smart card can be done at home through phone via OTA, at an ATM  
15 machine, at a service center or other convenient stores equipped with the appropriate,  
16 secured terminal. The distribution of the smart card can be handled through regular  
17 mail, so can the "refill" mechanism.

18 A unit amount, in dollars or minutes, representing purchased air time may be stored on  
19 a smart card. The user may make and receive phone calls, and use network services. The  
20 value on the smart card will be decremented as the authorized subscriber makes phone  
21 calls until the value of the card is exhausted. The subscriber may replenish the card by  
22 purchasing additional units. The service provider may offer a variety of rate plans and  
23 provision the smart card according to the subscriber's choice. After provisioning, the  
24 card value can only be decremented as phone calls are made.

25 The value of the card can only be incremented through an authorized party or process to  
26 avoid illegal tempering. The value filled in the smart card can be re-adjusted per  
27 subscriber's request through the pre-arranged authorization process supported by the  
28 service provider.

29 The smart card may be used to track value off-line, i.e. without network involvement.  
30 The subscriber may request to have balance and other relevant call detailed records  
31 displayed in the window provided on a mobile station.

32 Once the value on the smart card is depleted, the customer can not make normal phone  
33 calls except specified by the service provider. These allowable free calls can include 911  
34 emergency calls, 800 calls, or subscription related calls such as 411, 611, etc. to update  
35 the value and privileges carried by the card subscriber.

The smart card provisioning process, i.e., subscriber provisioning has to be automated with sufficient tools (OTASP and/or SIM application toolkit) to warrant an operation above and beyond the conventional existing plastic calling cards with or without the magnetic stripes. Manual operations to update individual subscriber databases are not acceptable by the service provider.

A subscriber scenario is described as follows: An automated kiosk at a neighborhood convenience store may accept cash, debit or credit cards in payment for added telecom units. The subscriber inserts cash or swipes a debit or credit card, indicates the value of the purchase, then receives a smart card for equal replenishment. Alternatively, the subscriber's service may be call-diverted to a customer service representative for the purchase of additional units. The customer service representative may replenish the smart card value via Over-the-Air Service Provisioning administration, or other automated procedures. The service provider can also mail the smart card to the subscriber for a newly established amount and a feature set.

The Pre-Paid Service should allow the service provider to better administer customer credit control, mass market penetration and acceptance of temporary or short term subscribers. This capability should make it possible for service providers to implement various billing strategies, such as mobile originated or mobile terminated limitations, as well as subscriber deletion without making major modifications to their networks. Eventually the smart card should carry individual billing information such as advice of charge.

Initially, a simplified Pre-paid Service with minimum impact on the network should be made available for the service provider to offer this service quickly. Later, a full capability of the Pre-paid service should be accommodated. This full capability is characterized as follows:

The residual value on a smart card should be dealt with fairly. A message should be delivered to the subscriber indicating insufficient value to make the next call. Options should be informed.

Examples of optional steps can be:

1. Call the service center to receive changes;
2. Call the service center to grant more value;
3. Enter a card terminal to receive value equivalent to additional cash payment;
4. Authorize usage of credit account to extend usage;
5. Receive a new card from a service center or in mail.

These options will be adopted according to the type of smart card as explained below:

1. Throwaway smart card. After credit amount and/or time expires, the smart card is permanently disposed of for making phone calls.

1                   2. Rechargeable smart card. The service provider can define circumstances by which  
2                   customers are able to recharge their smart cards with additional payments.

3                   3. Upgrade from prepaid to credit card. This will allow the subscriber to use post  
4                   payment service as it is typically the case after completing a successful credit check.

5

6                   Some tentative attributes and anticipated values are provided below:

Attribute	Value
Account balance	Assume \$0 - \$10,000, allowable per Service Provider
Rate set preferences	Assume maximum 100 rate plans
Accumulative call meter	
Advice of charge	
Currency exchange rate	Exchange rate of major currencies
OTASP	Over the Air Service Provisioning
DMH link	Tie to the near real time billing data
CHV Authorization	CHV, ESN and MIN combination

7

8                   5.1.1. Normal Procedures With Successful Outcome

9                   5.1.1.1. Authorization

10                  11 Pre-paid Service may be provided after pre-arrangement with the service provider, or  
may be made generally available by the service provider.

12

5.1.1.2. De-Authorization

13                  14

If Pre-paid Service is provided after pre-arrangement with the service provider, the service shall be de-authorized at the subscriber's request or for administrative reasons.

15

5.1.1.3. Registration

16                  17

Pre-paid Service should allow registration of the smart card either through the terminal/mobile station or through the network.

1                   **5.1.1.4. De-Registration**

---

2                   Pre-paid Service does not have to have De-Registration.

3                   **5.1.1.5. Activation**

---

4                   Pre-paid Service shall be activated upon authorization.

5                   **5.1.1.6. Deactivation**

---

6                   Pre-paid Service shall be de-activated upon De-Authorization.

7                   **5.1.1.7. Invocation**

---

8                   Pre-paid Service is invoked by issuing of the appropriate application level commands.

9                   **5.1.2. Exception Procedures or Unsuccessful Outcome**

---

10                  If the card is warped or damaged, the card can not trigger any service, replacement will  
11                  be sought. If card access by an unauthorized user is detected through CHV or other  
12                  security verification, the call will be denied.

13                  **5.1.2.1. Registration**

---

14                  None identified.

15                  **5.1.2.2. De-Registration**

---

16                  None identified.

17                  **5.1.2.3. Activation**

---

18                  None Identified.

19                  **5.1.2.4. Deactivation**

---

20                  None Identified.

21                  **5.1.2.5. Invocation**

---

22                  If Pre-paid Service cannot be established for the service session or if the service sessions  
23                  are interrupted in progress, the network may clear the service session. The originator of  
24                  the service session should be provided with an indication that the service session has  
25                  failed.

1

#### **5.1.2.6. Exceptions While Roaming**

---

2

None identified.

3

#### **5.1.2.7. Exceptions During Intersystem Hand-off**

---

4

Intersystem hand-off should not affect Pre-paid Service integrity.

5

#### **5.1.3. Alternate Procedures**

---

6

None identified.

7

#### **5.1.4. Interactions With Other Wireless Services**

---

8

##### **5.1.4.1.**

---

9

For Further Study

1

## 2 5.2. Plastic Roaming Service

---

3 Plastic Roaming Service will allow a user to roam outside of his/her home system  
4 through the use of a smart card. This service will provide the capability of allowing the  
5 user to authenticate with a preferred roaming system which has been previously defined  
6 on the smart card.

7 The smart card will contain a list of preferred serving systems that would associate the  
8 name/greeting of the service provider the subscriber is roaming on. When a subscriber  
9 selects a preferred serving system, the name and greeting of the local service provider  
10 may be delivered to the subscriber. This list will provide the subscriber greater  
11 flexibility of maintaining his/her most frequently visited location.

12 A smart card service provider may issue provided support of multiple technology  
13 imprinted on the card. The service provider that has more than one type of technology  
14 to offer to its cellular or PCS subscribers will have the capability of providing extended  
15 roaming access on the same smart card. If a smart card subscriber is unable to access a  
16 particular network technology, he/she may choose to disconnect from the network and  
17 reconnect with another network technology.

18 The smart card must be inserted into a smart card terminal unit at all times while plastic  
19 roaming. The smart card prepersonalization data must be verified and validated before  
20 plastic roaming can occur. After registration the service provider may access the  
21 roamer service profile. The roamer service profile may store and maintain the specific  
22 feature information (e.g. automatic roaming, NDSS, etc.) for call origination and  
23 termination

24 Smart card location information and time of call would provide geographical roaming  
25 information for call origination and termination. These characteristics should be used to  
26 facilitate billing functions via the home service provider.

27 Ultimately, the smart card should allow roaming across multiple bands (800, 900, 1800,  
28 1900 MHz, etc.) and multiple access technologies (PCS, CDMA, GSM, AMPS, TDMA  
29 etc.)

30

Attribute	Value
Prepersonalization data	Authentication key, IMSI, status of card(block, unblock), CHV
IMSI	International Mobile Station Identification
TMSI	Temporary Mobile Station Identification
LAI	Location Area Information (SID/NID)
Time	Time related to periodic location updating
Roamer Service Profile	Automatic roaming, SSPR, NDSS, CW, CFB, 3WC, etc.
Extended Network Technology Access	Provide interoperability with other networks (GSM, CDMA, PCS, AMPS, TDMA)
OTASP	Over the Air Service Provisioning
SID/NID	List of preferred Systems/Network ID provided by the home system
Feature Codes	Automatic roaming, SSPR, NDSS

1

2

### 5.2.1. Normal Procedures With Successful Outcome

---

3

#### 5.2.1.1. Authorization

---

4  
5  
6

Plastic Roaming Service may be provided after pre-arrangement with the service provider, or may be made generally available by the service provider. The smart card subscriber prepersonalization data would be imprinted on the card at authorization.

7

#### 5.2.1.2. De-Authorization

---

8  
9  
10

If Plastic Roaming Service is provided after pre-arrangement with the service provider, the service shall be de-authorized at the subscriber's request or for administrative reasons.

11

#### 5.2.1.3. Registration

---

12

Plastic Roaming Service has no registration. The mobile station handles registration.

1                   **5.2.1.4. De-Registration**

---

2                   Plastic Roaming Service has no De-Registration.

3                   **5.2.1.5. Activation**

---

4                   Plastic Roaming Service shall be activated upon authorization.

5                   **5.2.1.6. Deactivation**

---

6                   Plastic Roaming Service shall be de-activated upon De-Authorization.

7                   **5.2.1.7. Invocation**

---

8                   Plastic Roaming Service is invoked by the smart card user inserting the smart card into  
9                   the mobile station or smart card compatible device. The user may enter a CHV for  
10                  verification to access the smart card roamer service profile and other applications.

11                  **5.2.2. Exception Procedures or Unsuccessful Outcome**

---

12                  **5.2.2.1. Registration**

---

13                  None identified.

14                  **5.2.2.2. De-Registration**

---

15                  None identified.

16                  **5.2.2.3. Activation**

---

17                  None Identified.

18                  **5.2.2.4. Deactivation**

---

19                  None Identified.

20                  **5.2.2.5. Invocation**

---

21                  If Plastic Roaming Service cannot be established for the service session or if the service  
22                  sessions are interrupted in progress, the network may clear the service session. The  
23                  originator of the service session should be provided an indication that the service session  
24                  has failed.

1

#### **5.2.2.6. Exceptions While Roaming**

---

2

3

4

5

6

If plastic roaming service cannot be established or a service session fails while roaming, the originator has the option of reconnecting to another extended network technology. Reconnection would occur after the originator has disconnected from the current extended network technology he/she is on and re-register with another extended network.

7

#### **5.2.2.7. Exceptions During Intersystem Hand-off**

---

8

Intersystem hand-off should not affect Plastic Roaming Service integrity.

9

#### **5.2.3. Alternate Procedures**

---

10

None identified.

11

#### **5.2.4. Interactions With Other Wireless Services**

---

12

##### **5.2.4.1.**

---

13

For Further Study

14

## 5.3. Fraud Prevention Service

The smart card provides mechanisms that assure a high degree of privacy and authentication. This privacy and authentication function is the basis for all other smart card services. This function should be compliant with the existing UIM authentication and privacy specification for the PCS applications (ref. T1P1.3.)

The Fraud Prevention Service provides the following measures:

1. Preventing cloning of subscriptions by:

- Securing the distribution of subscriber data
- Secure storage on the smart card
- No programming of phone (at distribution) with sensitive data.

2. Authentication:

- User to SIM (subscription) with CHV/PIN
- SIM (subscription) to network with secret keys and algorithms

3. Safeguarding subscriber anonymity because:

- The average interceptor cannot tell who is using the phone (TIMSI), nor can the interceptor track the user.

4. Encryption of:

- all signaling data and
- all communications content (voice, data, etc.)

The smart card will handle multiple security algorithms including IS-41 and GSM based algorithms.

The smart card will be used in conjunction with the conventional CHV code. Subscriber fraud should be drastically reduced with the smart card due to the fact that the keys and the algorithm execution is performed within a secure environment of a single chip. At no time does secret data or intermediate algorithmic results leave this secure environment.

The smart card authentication will be handled either by the network or the compatible terminal/mobile station. The smart card needs to operate with networks that can/will handle authentication as well as those that can/will not. Depending on the network authentication capability, the proper combination of the CHV, A-key, MIN (or IMSI) and the ESN of the mobile station will be validated for a particular subscriber to assure maximum authentication. The subscriber security identity is portable with the card and the subscriber across all smart card capable mobile stations.

The smart card will enable the service provider to process authentication key with secured distribution and management. It should complement security functions supplied by the OTASP.

Attribute	Value
<b>Authentication key</b>	
<b>Authentication algorithm</b>	
<b>OTASP authentication responses</b>	

1

2

3

### 5.3.1. Normal Procedures With Successful Outcome

4

#### 5.3.1.1. Authorization

5  
6

Fraud Prevention Service may be provided after pre-arrangement with the service provider, or may be made generally available by the service provider.

7

The three categories of Fraud Prevention may be authorized as follows:

8  
9  
10  
11  
12

1. CHV code, is initially always enabled. The user can disable and enable this service at will. However pre-paid cards will always need a CHV code before attempting a call setup. The CHV will be administrated by the service provider in conjunction with different levels of security. The subscriber can access and change only the CHV, not other security algorithms involving A-key, etc.

13  
14

2. Authentication is mandatory. The A-key or similar parameters may be stored on a UIM together with an authentication algorithm.

15  
16

3. Encryption prevents subscription data from being illegally captured and used. Encryption shall always be used whenever available.

17

#### 5.3.1.2. De-Authorization

18  
19  
20  
21

If Fraud Prevention Service is provided after pre-arrangement with the service provider, the service shall be de-authorized at the subscriber's request or for administrative reasons. The Fraud Prevention Service is provided until termination of entire telephone service at the subscriber's request or for administrative reasons.

1

2 **5.3.1.3. Registration**

---

3 Fraud Prevention Service has no registration.

4 **5.3.1.4. De-Registration**

---

5 Fraud Prevention Service has no De-Registration

6 **5.3.1.5. Activation**

---

7 Fraud Prevention Service shall be activated upon authorization.

8 **5.3.1.6. Deactivation**

---

9 Fraud Prevention Service shall be de-activated upon De-Authorization.

10 **5.3.1.7. Invocation**

---

11 Fraud Prevention Service is invoked by issuing of the appropriate application level  
12 commands.

13 The three categories Fraud Prevention will be invoked:

14 1. CHV code is invoked by issuing of the appropriate application level commands.

15 2. Authentication is invoked by the MS or by the network.

16 3. Encryption is invoked by issuing of the appropriate application level commands.

17 **5.3.2. Exception Procedures or Unsuccessful Outcome**

---

18 **5.3.2.1. Registration**

---

19 None identified.

20 **5.3.2.2. De-Registration**

---

21 None identified.

22 **5.3.2.3. Activation**

---

23 None Identified.

#### 5.3.2.4. Deactivation

**2** None Identified.

### 5.3.2.5. Invocation

4 If Fraud Prevention Service cannot be established for the service session or if the service  
5 sessions are interrupted in progress, the network may clear the service session. The  
6 originator of the service session should be provided an indication that the service session  
7 has failed.

### 5.3.2.6. Exceptions While Roaming

9 None identified.

### 5.3.2.7. Exceptions During Intersystem Hand-off

11 Intersystem hand-off should not affect the Fraud Prevention Service integrity.

### 5.3.3. Alternate Procedures

13 None identified.

#### 5.3.4. Interactions With Other Wireless Services

#### 5.3.4.1.

16 Fraud Prevention Service is the foundation block to all the other services. This service  
17 will interact with other services at the beginning of the call set-up. More study is  
18 necessary.

## 5.4. Future Services

### 5.4.1. Portable Storage Service

Mapping of feature codes and other subscriber specific data to more user-friendly interface can be done in the smart card. Data stored in the smart card can be carried with the subscriber for activation in other location, device, or network. Examples of these data are listed below:

- 1) Translation of 911 to the number appropriate for a specific geographic location.
- 2) Service provider's name/greeting associated with certain SID/NID. When subscriber places a call in a new SID/NID, name and greeting of the local service provider can be delivered to the subscriber.
- 3) Voice print of the subscriber.
- 4) Audio characteristics.
- 5) Short messages, voice and facsimile messages delivered to the subscriber.
- 6) Personal health data, education and entertainment preferences.
- 7) Business specific application of data per employee, e.g. dispatch route assignments for driver X, etc.

Attribute	Value
Feature codes	
SID/NID list	
Voice print	
Audio signature	
Short messages	
Voice messages	
Facsimile messages	
Route information	
Personal health record	
Entertainment data	
OTASP	
CHV	

1

## 2 5.4.2. Non-telephony Services

---

3 Many current and proposed smart card applications address industries and consumer  
4 needs outside of telephony. A link to these services can be provided by the smart card  
5 which will allow telephony and non-telephony applications to co-exist on the same card.  
6 For example:

7 1) Transparent wireless transport for "end-to-end" applications facilitating interaction  
8 between the smart card and another entity, e.g. a host machine.

9 2) Business alliance between financial institution and the wireless service provider can  
10 link telephony and credit services via the smart card.

11 A telephony application on the smart card may provide wireless access to supply  
12 communication needs of another application also on that smart card. However, a number  
13 of these applications rely upon some form of transport to enable communications with a  
14 host application or database. For example, a financial services smart card enabling  
15 banking transactions might require access to host applications for funds transfer,  
16 payment and account updates. A multi-application smart card containing both a  
17 financial services and wireless services application could provide the required  
18 communications transport services. The user inserts the smart card into the mobile  
19 station, enters the appropriate CHV, then selects the desired financial services  
20 application from an application menu. User information and transaction data could be  
21 transmitted via SMS, voice or data channel from the smart card to the recipient  
22 application and vice versa. The user physically interacts only with the mobile station.

Attribute	Value
Application name	
Transport protocol	
CHV	
Application detailed billing	
SMS	

23

---

